UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,903	09/12/2003	Haixiang He	120-161	8338

34845 7590 03/19/2007
McGUINNESS & MANARAS LLP
125 NAGOG PARK
ACTON, MA 01720

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,903	HE ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/9/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of domestic priority under 35 U.S.C. 119(e) is acknowledged.

The application is filed on 9/12/2003 but has a U.S. provisional application number 10/442,657 filed on 1/24/2003.

Claim Objections

2. Claim 9 is objected to because of the following informalities: "the routing protocol of the background" should be "the routing protocol of the backbone". Appropriate correction is required.

Double Patenting

The nonstatutory provisional double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double

patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1 – 4 and 11 are rejected under the judicially created doctrine of obviousness-type provisional double patenting as being unpatentable over claims 1 – 4, 12 – 15 and 23 – 26 of copending application 10/661,657. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1 – 4 and 11 of the instant application are envisioned by the claims of the copending application that contain all the limitations of claims of the instant application such as encapsulating, transforming and updating a packet protocol between a first and second member of a private network over a backbone is obviously covered by the functions of appending, transforming and apportioning a packet protocol between a first and second member of a private network over a backbone and thereby, claims of the instant application are not patently distinct from the earlier copending application claim and as such are unpatentable for obvious-type provisional double patenting.

Likewise, claim 11 of the instant application is rejected under the judicially created doctrine of obviousness-type provisional double patenting as being unpatentable over claim 23 of copending application 10/661,657 with the similar reasons.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11 is indefinite because "an apparatus" is recited in the claim preamble; however, the claim limitations such as "a key table", tunneling mechanism" and "transform logic" can be implemented in hardware, software or some combination, according to the specification (SPEC: Page 18 Line 5 – 11), and thereby the claim may be reasonably interpreted as being not limited to hardware elements and the claim may be merely directed to software per se. Therefore, it is unclear and ambiguous with "an apparatus" being recited in the claim preamble. Besides, the claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to software per se which is directed to non-statutory subject matter.

Similar rationale of rejections can also apply to claim 13. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2 and 4 – 15 are rejected under 35 U.S.C. 102(e) as being anticipated by **Liu** (U.S. Patent 2002/0154635) which incorporates the reference of **Caronni** et al. (U.S. Patent 6,970,941) as shown in (Liu: Para [0002]).

As per claim 1, Liu / Caronni teaches a method of securing packet data transferred between a first and second member of a private network over a backbone, the backbone operating according to a routing protocol (Caronni : Column 2 Line 14 – 35 and Column 4 Line 38 – 52: "tunneling" refers to encapsulating one packet inside another when packets are transferred between two end points to ensure that the communication between itself and enterprise network is secure in that it cannot be viewed by an interloper), the method comprising the steps of:

encapsulating a private address of a packet from the first member in a public address of the packet to generate a tunneled packet (Caronni : Figure 2B & 6 / Element 640, Column 2 Line 30, Column 7 Line 10 – 20, Column 4 Line 40 – 60 and Column 6 Line 6 – 8: node ID is a private address and the real IP address is the public address);

transforming the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then updating a field in the secure tunneled packet in accordance with the routing protocol of the backbone (Caronni : Column 6 Line 12 – 16, Column 7 Line 5 –

33, Column 3 Line 17 – 21 and Column 11 Line 37 – 43: VARPDB stores the mappings of the internal / private address, known as node ID, which is considered as a part of the group security association and the Supernet contains a modification to the IP packet format that can be used to separate network behavior from addressing or the destination address becomes the real public-network destination address w.r.t the routing protocol of the backbone).

As per claim 9, Liu / Caronni teaches a method of securing packet data transferred between a first and second member of a private network over a backbone, the backbone operating according to a routing protocol (Caronni : Column 2 Line 14 – 35 and Column 4 Line 38 – 52: "tunneling" refers to encapsulating one packet inside another when packets are transferred between two end points to ensure that the communication between itself and enterprise network is secure in that it cannot be viewed by an interloper), the method comprising the steps of:

determining routing information associated with a packet received at the backbone according to the routing protocol of the backbone (Liu: Para [0070], Para [0050] and Para [0066] Line 1 – 4 / Line 8 – 10 and Figure 3 / Element 324 & Figure 6 and Caronni : Column 8 Line 31 – 37: the router node);

determining whether the packet is a member of the private network (Liu: Para [0070]); and

modifying at least one field of the packet according to a routing protocol of the private network responsive to a determination that the packet is a member of the private

network (Liu : Para [0070] and Para [0073] Line 7 – 9 & Caronni : Column 4 Line 56 – 59: upon a router receiving a packet, the forwarding destination node address will become a node ID of the Supernet (i.e. w.r.t. a protocol of the private network) or a modification to the IP packet format can be used to separate network behavior from addressing).

As per claim 11, Liu / Caronni teaches an apparatus at a node for transforming packets for forwarding between a plurality of members over a backbone in a scalable private network, wherein the backbone operates according to a protocol (Caronni : Column 2 Line 14 – 35 and Column 4 Line 38 – 52: "tunneling" refers to encapsulating one packet inside another when packets are transferred between two end points to ensure that the communication between itself and enterprise network is secure in that it cannot be viewed by an interloper), the apparatus comprising:

a key table, the key table including a security association for each private network that the node is a member (Caronni : Column 7 Line 5 – 33 : VARPDB stores the mappings of the internal / private address, known as node ID, which is considered as a part of key table);

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address to provide a secured packet (Caronni : Figure 2B & 6 / Element 640, Column 2 Line 30, Column 7 Line 10 – 20, Column 4 Line 40 – 60 and Column 6 Line 6 – 8: node ID is a private address and the real IP address is the public address);

transform logic operable to apply a security association to each packet transmitted to the backbone, the transform logic including means for updating a field of the secure packet in accordance with a protocol of the backbone (Caronni : Column 6 Line 12 – 16, Column 7 Line 5 – 33, Column 3 Line 17 – 21 and Column 11 Line 37 – 43: VARPDB stores the mappings of the internal / private address, known as node ID, which is considered as a part of the group security association and the Supernet contains a modification to the IP packet format that can be used to separate network behavior from addressing or the destination address becomes the real public-network destination address w.r.t the routing protocol of the backbone).

As per claim 13, Liu / Caronni teaches a provider node in a backbone of a scalable private network, for transforming packets forwarded between a plurality of members of the scalable private network over the backbone, wherein the backbone operates according to a protocol (Caronni : Column 2 Line 14 – 35 and Column 4 Line 38 – 52 & Liu: Para [0050]: "tunneling" refers to encapsulating one packet inside another when packets are transferred between two end points to ensure that the communication between itself and enterprise network is secure in that it cannot be viewed by an interloper), the provide node comprising:

a routing table, operable to determine a next hop routing address for each packet received at the provider node, the routing table operating responsive to a field of the packet arranged according to the protocol of the backbone (Liu: Para [0070], Para [0050] and [0066] Line 1 – 4 / Line 8 – 10 and Figure 3 / Element 324 & Figure 6 and

Caronni : Column 8 Line 31 – 37: the router node must be operable to determine a next hop routing address responsive to an "address" field of the packet based on a routing table); and

means for updating a field of the packet prior to the routing of the packet if it is determined that the packet is forwarded between members of the scalable private network (Liu : Para [0070] and Para [0073] Line 7 – 9 & Caronni : Column 4 Line 56 – 59: upon a router receiving a packet, the forwarding destination node address will become a node ID of the Supernet (i.e. w.r.t. a protocol of the private network) or a modification to the IP packet format can be used to separate network behavior from addressing).

As per claim 15, Liu / Caronni teaches a system for providing secure packet transmission between members of a scalable private network over a backbone comprising (Caronni : Column 2 Line 14 – 35 and Column 4 Line 38 – 52 & Liu: Para [0050]: "tunneling" refers to encapsulating one packet inside another when packets are transferred between two end points to ensure that the communication between itself and enterprise network is secure in that it cannot be viewed by an interloper), the system comprising:

a first node, coupled to a backbone, the first node being a member of the private network (Caronni : Para [0047]) and comprising:

a table for storing a group security association associated with the private network (Caronni : Column 7 Line 5 – 33 : VARPDB stores the mappings of the internal / private address, known as node ID, which is considered as a part of key table);

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address to provide a secured packet (Caronni : Figure 2B & 6 / Element 640, Column 2 Line 30, Column 7 Line 10 – 20, Column 4 Line 40 – 60 and Column 6 Line 6 – 8: node ID is a private address and the real IP address is the public address);

transform logic operable to apply a security association to each packet transmitted to the backbone, the transform logic including means for updating a field of the secure packet in accordance with a protocol of the backbone (Caronni : Column 6 Line 12 – 16, Column 7 Line 5 – 33, Column 3 Line 17 – 21 and Column 11 Line 37 – 43: VARPDB stores the mappings of the internal / private address, known as node ID, which is considered as a part of the group security association and the Supernet contains a modification to the IP packet format that can be used to separate network behavior from addressing or the destination address becomes the real public-network destination address w.r.t the routing protocol of the backbone); and

a provider node (Liu: Para [0050] and Para [0066] Line 1 – 4 / Line 8 – 10 and Figure 3 / Element 324 & Figure 6 and Caronni : Column 8 Line 31 – 37: the router node) in the backbone operating according to a routing protocol, the provider node comprising:

a routing table, operable to determine a next hop routing address for each packet received at the provider node, the routing table operating responsive to a field of the packet arranged according to the protocol of the backbone (Liu: Para [0070], Para [0050] and [0066] Line 1 – 4 / Line 8 – 10 and Figure 3 / Element 324 & Figure 6 and Caronni : Column 8 Line 31 – 37: the router node must be operable to determine a next hop routing address responsive to an "address" field of the packet based on a routing table); and

means for updating a field of the packet prior to the routing of the packet if it is determined that the packet is forwarded between members of the scalable private network (Liu : Para [0070] and Para [0073] Line 7 – 9 & Caronni : Column 4 Line 56 – 59: upon a router receiving a packet, the forwarding destination node address will become a node ID of the Supernet (i.e. w.r.t. a protocol of the private network) or a modification to the IP packet format can be used to separate network behavior from addressing).

As per claim 2, Liu / Caronni teaches the backbone comprises a plurality of provide devices (Liu: Page 2 Line 1 – 2), and wherein the steps of encapsulating and transforming are performed at one of the plurality of provider devices (Liu: Para [0050] Line 3 – 7, Para [0065] Line 4 – 7, Para [0066] Line 1 – 4 / 8 – 10 and Caronni : Column 8 Line 31 – 47: alternatively, the router node, by running SNlogin, can perform address translation and security encapsulation transparently the same way as the computer terminal device node does).

As per claim 4, Liu / Caronni teaches the steps of encapsulating and transforming are performed at the first member (Caronni : Column 2 Line 27 – 32: terminal computer device D_1).

As per claim 5 and 12, Liu / Caronni teaches the step of updating the field in the secure tunnel packet replaces a destination field associated with the private network with a destination field associated with the routing protocol of the backbone (Caronni : Figure 6 / Element 616, Column 6 Line 12 – 16: the real public-network destination address w.r.t the routing protocol of the backbone).

As per claim 6, Liu / Caronni teaches the group security association is associated with each member of the private network (Caronni : Column 7 Line 5 – 33, Column 3 Line 17 – 21 and Column 11 Line 37 – 43: VARPDB stores the mappings of the internal / private address, known as node ID, which is considered as part of a group security association).

As per claim 7, Liu / Caronni teaches each member of the private network registering with a global security server; the global security server forwarding the group security association to each member of the private network (Caronni : Column 7 Line 64 – 67: KMS = Key Management Server : generating a new key and forwarding to each member of the private network).

As per claim 8, Liu / Caronni teaches the global security server periodically forwarding a new group security association to each member of the private network (Caronni : Column 12 Line 3: updated every ten seconds).

As per claim 10 and 14, Liu / Caronni teaches modifying replaces a destination field associated with the routing protocol of the backbone with a destination field associated with a protocol of the private network (Liu : Para [0070] and Para [0073] Line 7 – 9 & Caronni : Column 4 Line 56 – 59: upon a router receiving a packet, the forwarding destination node address will become a node ID of the Supernet (i.e. w.r.t. a protocol of the private network) or a modification to the IP packet format can be used to separate network behavior from addressing).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liu (U.S. Patent 2002/0154635), in view of Alkhatib et al. (U.S. Patent 2003/0233454).

As per claim 3, Liu does not disclose expressly encapsulating and transforming are performed at an edge device disposed between the first member and the backbone.

Alkhatib teaches encapsulating and transforming are performed at an edge device disposed between the first member and the backbone (Alkhatib : Par [0049] Line 14 – 17 and Para [0017] Line 1 – 8: a gateway, that changes and encapsulates the destination address, can be considered as an edge device, which also appears in the specification of the instant application (SPEC: Page 3 Line 14: Customer Edge device may also be referred to as a gateway device).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Alkhatib within the system of Liu because (a) Liu teaches a mechanism to extend private networks onto a public infrastructure (Liu: Para [0015] and [0018]) and (b) Alkhatib teaches providing a method to create a binding between public address and private address when communicating over a private network (Alkhatib : Para [0019]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
2/8/2007